Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method of communicating to a server machine a certificate of a user which is sent by a client machine via a security module of a computer system, wherein a first protocol used between the client machine and the server machine is a non-secure stateless protocol, and a second protocol used between the client machine and the security module is a secure stateless protocol, said method comprising:

transmitting said certificate from the client machine to said security module using said second secure stateless protocol;

inserting, said certificate unmodified into a cookie header of a request in the first non-secure stateless protocol, the inserting being done by the security module; and

transmitting the request, including said cookie header containing said certificate, from the security module to the server machine using said first non-secure protocol;

wherein said certificate has a plurality of separators; and

wherein said cookie header of said request includes a plurality of cookies.

2. (previously presented) A method according to claim 1, further comprising:

removing from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header of said request.

3. (previously presented) A method according to claim 1, wherein said inserting step further comprises:

determining, prior to the inserting step, whether an existing cookie header is present in the request sent by the client machine; and

creating a new cookie header if said existing cookie header is not present in the request sent by the client machine.

4. (previously presented) A method according to claim 3, further comprising:

adding a specific cookie into the existing or new cookie header; and

assigning a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.

5. (cancelled).

6. (currently amended) An apparatus comprising:

a security machine configured to secure exchanges between a client machine and a server machine of a computer system, wherein a first protocol used between the client machine and server machine is a non-secure stateless protocol, and a second protocol implemented between the client machine and said security machine is a secure stateless protocol,

wherein said security machine further comprises an analyzer configured to insert an unmodified certificate received from the client machine using said second secure stateless protocol into a cookie header of an HTTP or equivalent request, and further configured to transmit to a server said unmodified certificate contained in said cookie header using said first non-secure stateless protocol; and

wherein said cookie header of said request includes a plurality of cookies.

7. (currently amended) A system comprising:

a client machine;

a server machine; and

a security module interposed between the client machine and the server machine and provided in communication therewith;

wherein the client machine and the server machine are configured to communicate using a first protocol, said first protocol comprising a non-secure stateless protocol;

wherein the client machine and the security module are configured to communicate using a second protocol, said second protocol comprising a secure stateless protocol; and

wherein the security module comprises an analyzer configured to insert an unmodified certificate sent by the client machine into a cookie header of a request in conformance with said non-secure stateless protocol, and wherein the analyzer is further configured to transmit to a server said unmodified certificate contained in said cookie header using said non-secure stateless protocol, said cookie header of said request including a plurality of cookies.

8. (currently amended) One or more computer readable storage media upon which is encoded and stored a sequence of programmable instructions which, when executed by one or more processors, cause the processors to:

transmit a certificate of a user from a client machine to a security module ~~communicate to a server machine a certificate of a user which is sent by a client machine via a security module, wherein~~ using a secure stateless protocol ~~a firstprotocol used between the client machine and the server machine is a non-secure~~

~~stateless protocol, and wherein a second protocol used between the client machine and the security module is a secure stateless protocol~~;

insert at the security module said certificate unmodified into a cookie header of a request conforming to ~~the first~~ a non-secure stateless protocol; and

transmit the request, including said cookie header containing said unmodified certificate, from the security module to the server machine using ~~said first~~ the non-secure stateless protocol;

wherein said certificate has a plurality of separators; and

wherein said cookie header of said request includes a plurality of cookies.

9. (previously presented) The computer-readable storage media of claim 8, further comprising instructions to:

remove from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header of said request.

10. (previously presented) The computer-readable storage media of claim 8, further comprising instructions to:

determine, prior to the inserting step, whether an existing cookie header is present in the request sent by the client machine; and

create a new cookie header if said existing cookie header is not present in the request sent by the client machine.

11. (previously presented) The computer-readable storage media of claim 10, further comprising instructions to:

add a specific cookie into the existing or new cookie header; and

assign a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.

12. (previously presented) The system of claim 7, wherein said analyzer is further configured to:

remove from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header of said request.

13. (previously presented) The system of claim 7, wherein said analyzer is further configured to:

determine, prior to said inserting, whether an existing cookie header is present in the request sent by the client machine; and

create a new cookie header if said existing cookie header is not present in the request sent by the client machine.

14. (previously presented) The system of claim 13, wherein said analyzer is further configured to:

add a specific cookie into the existing or new cookie header; and

assign a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.

15. (previously presented) The apparatus of claim 6, wherein said security machine is further configured to:

remove from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header of said request.

16. (previously presented) The apparatus of claim 6, wherein said security machine is further configured to:

determine, prior to said inserting, whether an existing cookie header is present in the request sent by the client machine; and

create a new cookie header if said existing cookie header is not present in the request sent by the client machine.

17. (previously presented) The apparatus of claim 16, wherein said security machine is further configured to:

add a specific cookie into the existing or new cookie header; and

assign a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.